PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-163849
(43)Date of publication of application : 18.06.1999

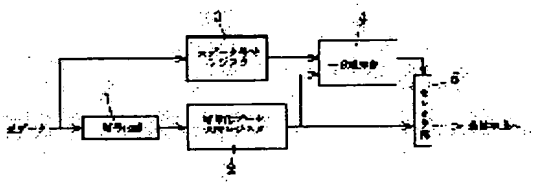
(51)Int.Cl. H04L 9/06
H04L 9/10
// G09C 1/00

(21)Application number : 09-323541
(22)Date of filing : 25.11.1997

(71)Applicant : MATSUSHITA ELECTRIC WORKS LTD
(72)Inventor : KAMIYANAGI HIDEKI

(54) ENCRYPTION COMMUNICATION METHOD AND ITS SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To enhance the security of encryption by precluding the possibility of decoding of encryption data.
SOLUTION: Original received data are given to an encryption coding section 1, where the data are encrypted according to a DES encryption algorithm and stored in an encryption data latch register 2. A coincidence detection section 4 detects whether or not the original data latched in an original data latch register 3 and encrypted data latched in the encryption data latch register 2 are coincident. In the case that the coincidence detection section 4 detects the coincidence of the original data and the encrypted data, a selector section 5 stops output of the coincident encryption data to prevent the encryption data coincident with the original data from being sent to a communication opposite party. As a result, the possibility of decoding of the encryption data is precluded to enhance the security of encryption.



LEGAL STATUS

[Date of request for examination] 10.08.2000
[Date of sending the examiner's decision of rejection] 06.04.2004
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号

特開平11－163849

(43)公開日　平成11年(1999)６月18日

(51)Int.Cl.[6]		識別記号	FI		
Ｈ０４Ｌ	9/06		Ｈ０４Ｌ	9/00	６１１Ａ
	9/10		Ｇ０９Ｃ	1/00	６１０Ｂ
// Ｇ０９Ｃ	1/00	６１０	Ｈ０４Ｌ	9/00	６２１Ｚ

審査請求　未請求　請求項の数６　ＯＬ　（全６頁）

(21)出願番号　特願平9－323541

(22)出願日　平成９年(1997)11月25日

(71)出願人　000005832
松下電工株式会社
大阪府門真市大字門真1048番地

(72)発明者　上柳　秀樹
大阪府門真市大字門真1048番地松下電工株式会社内

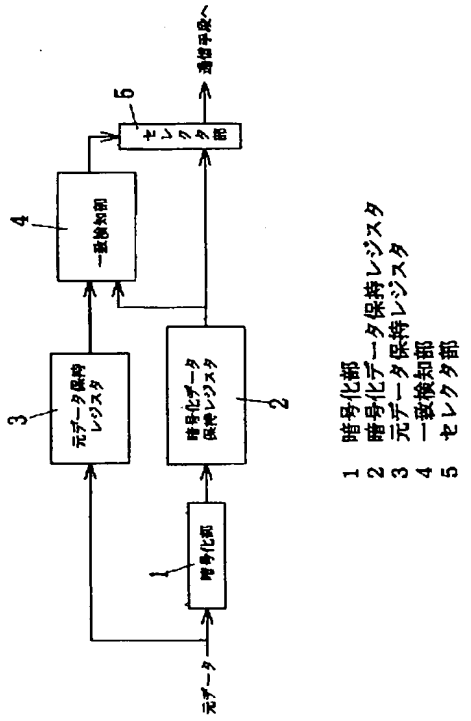
(74)代理人　弁理士　西川　惠清　（外１名）

(54)【発明の名称】　暗号通信方法及びその装置

(57)【要約】

【課題】暗号化データが解読される虞を小さくして暗号強度を高める。

【解決手段】入力される元データは暗号化部１にてＤＥＳの暗号アルゴリズムに従って暗号化され、暗号化データ保持レジスタ２に保持される。一致検知部４は、元データ保持レジスタ３に保持された元データと、暗号化データ保持レジスタ２に保持された暗号化データとが一致しているか否かを検知する。そして、一致検知部４にて元データと暗号化データの一致が検知された場合には、セレクタ部４において当該一致した暗号化データの出力を停止することにより、元データと一致した暗号化データが通信相手に送信されるのを防止する。その結果、暗号化データが解読される虞を小さくして暗号強度を高めることができる。



1

【特許請求の範囲】

【請求項１】　暗号化と復号化とに共通の鍵を使用して暗号化データの通信を行う暗号通信方法において、暗号化される前の元データと暗号化された暗号化データとが一致しているか否かを検知し、一致している場合には当該暗号化データの送信を行わないことを特徴とする暗号通信方法。

【請求項２】　暗号化と復号化とに共通の鍵を使用して暗号化データの通信を行う暗号通信装置において、入力されるデータを所定の暗号アルゴリズムに従って暗号化する暗号化部と、暗号化部から出力される暗号化データと暗号化される前の元データとが一致するか否かを検知する一致検知部と、一致検知部にて元データと暗号化データとの一致が検知された場合に暗号化データの出力を停止するセレクタ部とを備えたことを特徴とする暗号通信装置。

【請求項３】　一致検知部は、元データと暗号化データの一致を検知した場合に暗号化部に元データを出力する手段に対して一致検知信号を出力することを特徴とする請求項２記載の暗号通信装置。

【請求項４】　一致検知部により元データと暗号化データの一致が検知された場合に通信相手に上記データの一致を通知する通知データを生成する通知データ生成部を備えたことを特徴とする請求項３記載の暗号通信装置。

【請求項５】　一致検知部により元データと暗号化データの一致が検知された場合に暗号化部で使用する共通鍵を変更する鍵変更部を備えたことを特徴とする請求項２又は３又は４記載の暗号通信装置。

【請求項６】　鍵変更部により共通鍵が変更されたことを通信相手に通知するための鍵変更通知データを生成する鍵変更通知データ生成部を備えたことを特徴とする請求項５記載の暗号通信装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、暗号化と復号化とに共通の鍵を使用する暗号化方式、特にＤＥＳ（Data Encryption Standard）を利用した暗号通信方法及びその装置に関するものである。

【０００２】

【従来の技術】従来より、データを暗号化して通信する場合に、アメリカ商務省標準局が１９７７年に公表したＤＥＳ（Data Encryption Standard）と呼ばれる、暗号化と復号化とに共通の鍵を使用する暗号アルゴリズムが用いられることが多い。上記ＤＥＳでは、６４ビットのデータブロック単位に暗号化及び復号化が行われ、鍵の長さは５６ビット（８ビットのパリティビットを加える６４ビット）とされている。この暗号アルゴリズムは転置と換字とを基本としており、これらの転置と換字を適当に組み合わせた処理を複数回繰り返すことにより、元データのビットパターンを変更して、元データと異なる暗号化データに変換している。暗号化データを復号する場合は、逆に変更することにより元データを復元することができる。而して、上記変更のパラメータを５６ビットの鍵（共通鍵）で指定するのである。

【０００３】

【発明が解決しようとする課題】ところで、上記暗号アルゴリズム（ＤＥＳ）においては、暗号化される前の元データと暗号化されたデータ（暗号化データ）のビットパターンが一致することが起こり得る。このように元データと暗号化データが一致した場合でも、従来はその暗号化データをそのまま通信相手に送信していた。

【０００４】一般に暗号化前後のデータが他人に知られると、そのデータの組から暗号化に使用した共通鍵を割り出す作業は、暗号化前後のデータの組が知られていない場合に比較してはるかに容易になる。従って、元データと暗号化データが一致してしまったときに、その一致した暗号化データをそのまま送信すると暗号化前後のデータの組が他人（盗聴者など）に知られ易くなり、そこから共通鍵が割り出されて通信される全てのデータが解読されてしまう虞が大きくなる。

【０００５】本発明は上記事情に鑑みて為されたものであり、その目的とするところは、暗号化データが解読される虞を小さくして暗号強度を高めた暗号通信方法及びその装置を提供することにある。

【０００６】

【課題を解決するための手段】請求項１の発明は、上記目的を達成するために、暗号化と復号化とに共通の鍵を使用して暗号化データの通信を行う暗号通信方法において、暗号化される前の元データと暗号化された暗号化データとが一致しているか否かを検知し、一致している場合には当該暗号化データの送信を行わないことを特徴とし、元データと暗号化データの組が他人に知られることがなく、暗号化データが解読される虞を小さくして暗号強度を高めることができる。

【０００７】請求項２の発明は、上記目的を達成するために、暗号化と復号化とに共通の鍵を使用して暗号化データの通信を行う暗号通信装置において、入力されるデータを所定の暗号アルゴリズムに従って暗号化する暗号化部と、暗号化部から出力される暗号化データと暗号化される前の元データとが一致するか否かを検知する一致検知部と、一致検知部にて元データと暗号化データとの一致が検知された場合に暗号化データの出力を停止するセレクタ部とを備えたことを特徴とし、元データと暗号化データの組が他人に知られることがなく、暗号化データが解読される虞を小さくして暗号強度を高めることができる。

【０００８】請求項３の発明は、請求項２の発明において、一致検知部が、元データと暗号化データの一致を検知した場合に暗号化部に元データを出力する手段に対して一致検知信号を出力することを特徴とし、上記手段に

データの通信が停止したことを知らせることができる。請求項４の発明は、請求項３の発明において、一致検知部により元データと暗号化データの一致が検知された場合に通信相手に上記データの一致を通知する通知データを生成する通知データ生成部を備えたことを特徴とし、通信相手にデータの通信が停止したことを知らせることができる。

【０００９】請求項５の発明は、請求項２又は３又は４の発明において、一致検知部により元データと暗号化データの一致が検知された場合に暗号化部で使用する共通鍵を変更する鍵変更部を備えたことを特徴とし、共通鍵を変更することで暗号化部におけるデータの暗号化処理が停止することを回避できる。請求項６の発明は、請求項５の発明において、鍵変更部により共通鍵が変更されたことを通信相手に通知するための鍵変更通知データを生成する鍵変更通知データ生成部を備えたことを特徴とし、共通鍵が変更されたことを通信相手に通知することができ、データの通信が停止することを回避できる。

【００１０】

【発明の実施の形態】（実施形態１）図１に本発明の実施形態１の要部ブロック図を示す。本実施形態の暗号通信装置は、図示しない前段の回路から入力される元データ（暗号化される前のデータ）をＤＥＳの暗号アルゴリズムに従って暗号化する暗号化部１と、暗号化部１で暗号化されたデータ（暗号化データ）を保持する暗号化データ保持レジスタ２と、元データを保持する元データ保持レジスタ３と、これら両レジスタ２，３に保持されている暗号化データと元データとが一致しているか否かを検知する一致検知部４と、暗号化データ保持レジスタ２から入力される暗号化データを次段の通信手段（無線や有線の通信回路など）に出力するとともに一致検知部４にて元データと暗号化データの一致が検知された場合には上記通信手段への当該一致した暗号化データの出力を停止するセレクタ部４とを備えている。

【００１１】一致検知部４は、例えば元データ保持レジスタ３に保持されている元データを読み出すとともに、暗号化データ保持レジスタ２に保持されている暗号化データを読み出し、データブロック単位に元データと暗号化データを比較して全てのビットが一致しているか否かを調べ、一致した場合にはその結果がセレクタ部５に送られる。

【００１２】一方、セレクタ部５には暗号化データ保持レジスタ２から暗号化データが入力されており、一致検知部４でデータの一致が検知されたなかった場合にはそのまま暗号化データを出力し、一致が検知された場合には暗号化データが送信されないような処理（例えば、次段の通信手段への暗号化データの出力を停止するなど）を行う。

【００１３】上述のように本実施形態によれば、一致検知部４にて元データの暗号化データが一致しているか否かを検知し、データの一致が検知された場合にはセレクタ部５により通信相手に一致した暗号化データが送信されないようにしているので、元データと暗号化データの組が他人に知られることがなく、暗号化データが解読される虞を小さくして暗号強度を高めることができる。しかも、ハードウェアを大幅に付加することなく上記機能が実現できるという利点がある。

【００１４】（実施形態２）図２に本発明の実施形態２の要部ブロック図を示す。本実施形態の基本構成は実施形態１と共通であり、共通する部分については同一の符号を付して説明を省略する。実施形態１では、一致検知部４で元データと暗号化データの一致が検知された場合にはその暗号化データの送信が停止されるのであるが、暗号化部１に元データを入力する前段の回路６では出力したデータの送信が停止されたことを知ることができず、その後の処理に支障を来す場合もある。

【００１５】そこで、本実施形態は、一致検知部４が元データと暗号化データの一致を検知した場合に暗号化部１に元データを出力する前段の回路６に対して一致検知信号を出力するようにし、前段の回路６に暗号化データの送信が停止されたことを知らせるようにした点に特徴がある。ここで、本実施形態においては、前段の回路６に対して暗号化データの送信停止を知らせる一致検知信号として、一致検知部４から出力される一致検知結果の信号を前段の回路６へフィードバックするようにしている。

【００１６】上述のように本実施形態では、元データを出力する前段の回路６に対して一致検知部４から元データと暗号化データが一致したときにその検知結果を知らせるようにしたので、前段の回路６においてはデータの通信停止に対応した適切な処理を行うことができるようになる。

（実施形態３）図３に本発明の実施形態３の要部ブロック図を示す。本実施形態の基本構成は実施形態１と共通であり、共通する部分については同一の符号を付して説明を省略する。

【００１７】実施形態１及び２では、一致検知部４で元データと暗号化データの一致が検知された場合にはその暗号化データの送信が停止されるのであるが、通信相手側ではデータの送信が停止されたことを知ることができず、その後の処理に支障を来す場合もある。そこで、本実施形態は、一致検知部４により元データと暗号化データの一致が検知された場合に、通信相手に上記データの一致を通知する通知データを生成する通知データ生成部７を備え、通信相手に対してデータの送信が停止されたことを知らせるようにした点に特徴がある。

【００１８】通知データ生成部７は、通信相手との間で予め決定されている所定の通知データ（暗号化されたデータであることが望ましい）を生成してセレクタ部５に出力する。一方、セレクタ部５は一致検知部４でデータ

の一致が検知されたなかった場合にはそのまま暗号化データを出力し、一致が検知された場合にはその暗号化データが送信されないような処理を行うとともに、通知データ生成部７で生成された通知データが通信相手に送信されるように次段の通信手段にその通知データを出力する。

【００１９】而して、通信相手側では通知データを受信することで暗号化データの送信が停止されたことを知ることができ、データの通信停止に対応した適切な処理を行うことができる。

（実施形態４）図４に本発明の実施形態４の要部ブロック図を示す。本実施形態の基本構成は実施形態１と共通であり、共通する部分については同一の符号を付して説明を省略する。

【００２０】実施形態１～３では、一致検知部４で元データと暗号化データの一致が検知された場合にはその暗号化データの送信されず、データの通信が一旦停止してしまい、その後の処理に支障を来す場合もある。そこで、本実施形態は、一致検知部４により元データと暗号化データの一致が検知された場合に、暗号化部１で使用する共通鍵を変更する鍵変更部８を備え、共通鍵を変更することで暗号化部１におけるデータの暗号化処理が停止することを回避するようにした点に特徴がある。

【００２１】鍵変更部８は、予め記憶されている複数の共通鍵の中から一致検知部４で一致が検知されたときに使用されていた共通鍵と異なる共通鍵を選択して暗号化部１に出力する。暗号化部１では暗号化に使用する共通鍵を鍵変更部８から出力されてくる共通鍵に変更し、あらためて元データの暗号化を行って暗号化データを出力する。

【００２２】上述のように本実施形態では、一致検知部４により元データと暗号化データの一致が検知された場合に、暗号化部１で使用する共通鍵を変更する鍵変更部８を備えたので、元データと暗号化データが一致した場合に再度異なる共通鍵を使用して元データを暗号化することにより、暗号化部１におけるデータの暗号化処理が停止することを回避できるという利点がある。

【００２３】なお、鍵変更部８で共通鍵が変更されてしまうと、通信相手側では変更前の共通鍵を使用しているために受信した暗号化データを復号化することができないが、例えば、電話などの別の通信手段を用いて通信相手側に変更された共通鍵を通知したり、あるいは予め変更候補の共通鍵を通信相手側にも保存しておき、受信した暗号化データが解読できない場合には変更候補の中から所定の共通鍵を選択して復号をやり直すようにすればよい。

【００２４】（実施形態５）図５に本発明の実施形態５の要部ブロック図を示す。本実施形態の基本構成は実施形態４と共通であり、共通する部分については同一の符号を付して説明を省略する。すなわち、本実施形態は鍵変更部８により共通鍵が変更されたことを通信相手に通知するための鍵変更通知データを生成する鍵変更通知データ生成部９を備えた点に特徴がある。

【００２５】鍵変更通知データ生成部９は、通信相手との間で予め決定されている所定の鍵変更通知データ（暗号化されたデータであることが望ましい）を生成してセレクタ部５に出力する。一方、セレクタ部５は一致検知部４でデータの一致が検知されたなかった場合にはそのまま暗号化データを出力し、一致が検知された場合にはその暗号化データが送信されないような処理を行うとともに、鍵変更通知データ生成部９で生成された鍵変更通知データが通信相手に送信されるように次段の通信手段にその鍵変更通知データを出力する。

【００２６】而して、通信相手側では、鍵変更通知データを受信すれば、例えば予め変更候補の共通鍵を保存しており、受信した鍵変更通知データに応じて変更候補の中から所定の共通鍵を選択して復号をやり直す。なお、鍵変更通知データとして変更後の共通鍵を通信相手に送信するようにしてもよい。上述のように本実施形態によれば、鍵変更部８により共通鍵が変更されたことを通信相手に通知するための鍵変更通知データを生成する鍵変更通知データ生成部９を備えたので、通信相手側で共通鍵の変更等の適切な処理を行って、データの通信が停止することを回避できるという利点がある。

【００２７】

【発明の効果】請求項１の発明は、暗号化と復号化とに共通の鍵を使用して暗号化データの通信を行う暗号通信方法において、暗号化される前の元データと暗号化された暗号化データとが一致しているか否かを検知し、一致している場合には当該暗号化データの送信を行わないので、元データと暗号化データの組が他人に知られることがなく、暗号化データが解読される虞を小さくして暗号強度を高めることができるという効果がある。

【００２８】請求項２の発明は、暗号化と復号化とに共通の鍵を使用して暗号化データの通信を行う暗号通信装置において、入力されるデータを所定の暗号アルゴリズムに従って暗号化する暗号化部と、暗号化部から出力される暗号化データと暗号化される前の元データとが一致するか否かを検知する一致検知部と、一致検知部にて元データと暗号化データとの一致が検知された場合に暗号化データの出力を停止するセレクタ部とを備えたので、元データと暗号化データの組が他人に知られることがなく、暗号化データが解読される虞を小さくして暗号強度を高めることができるという効果がある。

【００２９】請求項３の発明は、一致検知部が、元データと暗号化データの一致を検知した場合に暗号化部に元データを出力する手段に対して一致検知信号を出力するので、上記手段にデータの通信が停止したことを知らせることができるという効果がある。請求項４の発明は、一致検知部により元データと暗号化データの一致が検知

された場合に通信相手に上記データの一致を通知する通知データを生成する通知データ生成部を備えたので、通信相手にデータの通信が停止したことを知らせることができるという効果がある。

【００３０】請求項５の発明は、一致検知部により元データと暗号化データの一致が検知された場合に暗号化部で使用する共通鍵を変更する鍵変更部を備えたので、共通鍵を変更することで暗号化部におけるデータの暗号化処理が停止することを回避できるという効果がある。請求項６の発明は、鍵変更部により共通鍵が変更されたことを通信相手に通知するための鍵変更通知データを生成する鍵変更通知データ生成部を備えたので、共通鍵が変更されたことを通信相手に通知することができ、データ

の通信が停止することを回避できるという効果がある。

【図面の簡単な説明】

【図１】実施形態１の要部を示すブロック図である。

【図２】実施形態２の要部を示すブロック図である。

【図３】実施形態３の要部を示すブロック図である。

【図４】実施形態４の要部を示すブロック図である。

【図５】実施形態５の要部を示すブロック図である。

【符号の説明】

１　暗号化部

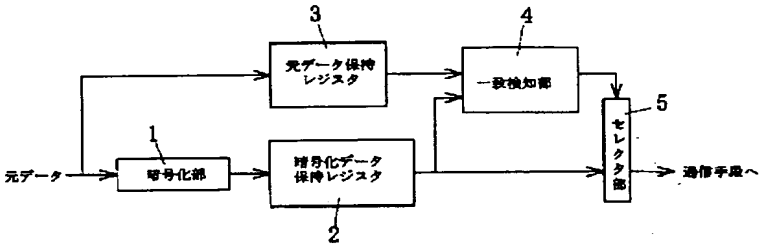
２　暗号化データ保持レジスタ

３　元データ保持レジスタ

４　一致検知部

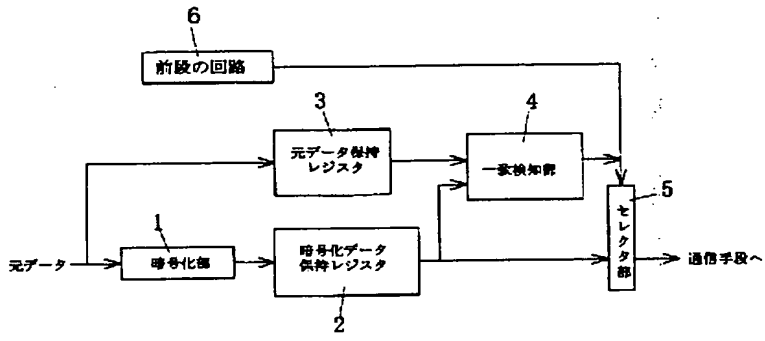
５　セレクタ部

【図１】

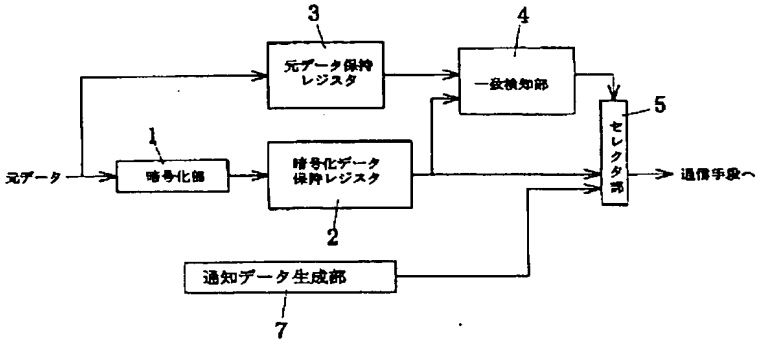


１　暗号化部
２　暗号化データ保持レジスタ
３　元データ保持レジスタ
４　一致検知部
５　セレクタ部

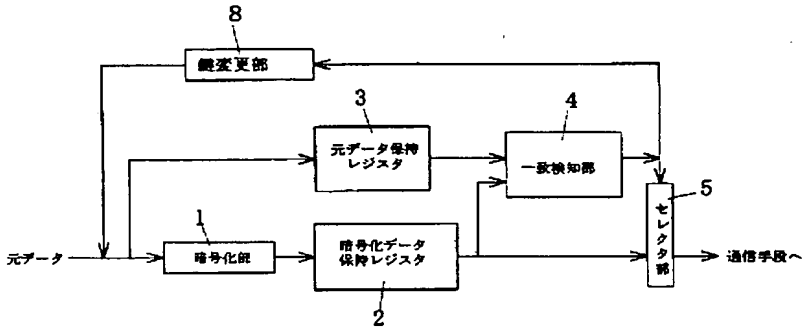
【図２】



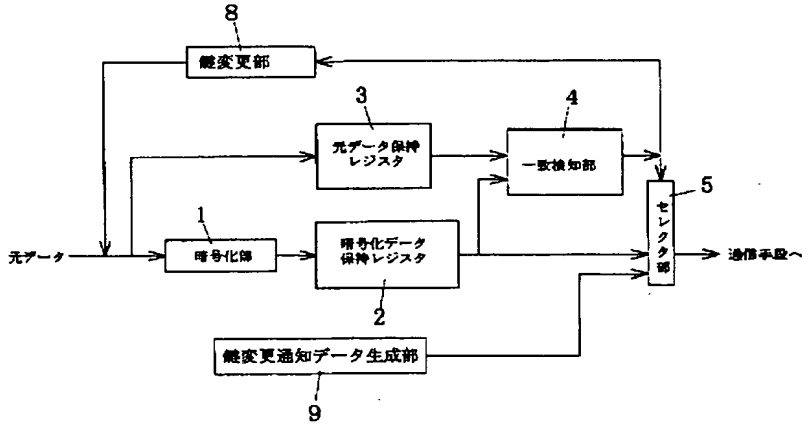
【図３】


3
元データ保持レジスタ
4
一致検知部
5
セレクタ部
1
暗号化部
暗号化データ保持レジスタ
2
元データ
通信手段へ
通知データ生成部
7

【図４】


8
鍵変更部
3
元データ保持レジスタ
4
一致検知部
5
セレクタ部
1
暗号化部
暗号化データ保持レジスタ
2
元データ
通信手段へ

【図５】


8
鍵変更部
3
元データ保持レジスタ
4
一致検知部
5
セレクタ部
1
暗号化部
暗号化データ保持レジスタ
2
元データ
通信手段へ
鍵変更通知データ生成部
9